جامعة دمشق

كلية الهندسة المعلوماتية

قسم النظم و الشبكات الحاسوبية

السنة الخامسة



Network Security

Digital Certificates & SSL

SSL والشهادات الرقمية

إعداد :

مصطفى محمد نجم

تمهيد :

المصادقة هامة لتوفير اتصال آمن. يجب أن يتمكن المستخدمون من إثبات هويتهم لمن يتصلون بهم ويجب أن يتمكنوا من التحقق من هوية الآخرين. تعتبر مصادقة هوية على شبكة اتصال عملية معقدة لأن الجهات المتصلة لا تتطابق فعلياً عند الاتصال. يمكن أن يسمح هذا لشخص غير أخلاقي بأن يحتجز الرسائل أو ينتحل صفة شخص أو كيان آخر.

الشهادة الرقمية هي ورقة اعتماد توفر وسيلة للتحقق من الهوية. تستخدم الشهادات تقنيات التشفير من أجل حل مشكلة افتقاد الاتصال الفعلي بين المتصلين. يحد استخدام هذه التقنيات من احتمال احتجاز الرسائل، أو تغييرها، أو تزييفها من قبل شخص غير أخلاقي. تؤدي تقنيات التشفير هذه إلى جعل الشهادات صعبة التعديل. وهكذا، سيكون من الصعب على أي شخص انتحال صفة شخص آخر .

تتضمن البيانات الموجودة في الشهادة مفتاح التشفير العمومي من زوج المفاتيح الخاص والعمومي لصاحب الشهادة. يمكن التحقق من أن الرسالة الموقعة باستخدام المفتاح الخاص للمرسل مصدقة وذلك من قبل مستلم الرسالة وباستخدام المفتاح العمومي للمرسل. يمكن العثور على هذا المفتاح على نسخة من شهادة المرسل. إن التحقق من التوقيع باستخدام المفتاح العمومي من شهادة يثبت أنه قد تم إنشاء هذا التوقيع باستخدام المفتاح الخاص لصاحب الشهادة. إذا كان المرسل حذراً وأبقى المفتاح الخاص سرياً، يمكن أن يثق المتلقي بهوية مرسل الرسالة.

طوَّرت شركة نتسكيب بروتوكول الطبقات الأمنية لتأمين نقل آمن للمعلومات بين خادم الويب ومستعرِضات الويب. ويعتمد هذا البروتوكول على خوارزمية المفتاح العام (public key) والمفتاح الخاص(private key) ، إذ يزوِّد الخادمُ المستفيدَ بالمفاتيحَ العامة، وتُستَخدَم هذه المفاتيح العامة في تشفير الرسائل المتَّجِهة إلى الخادم، ولا يمكن استخدام المفتاح العام لِفك شيفرة الرسالة التي شَفَّرها، إذ يتفرَّد المفتاح الخاص (لدى الخادم) بالقدرة على فك شيفرة الرسالة التي شفَّرَها المفتاح العام .

ويستطيع المستفيد (client) بالطريقة ذاتِها إنشاء زوج من المفاتيح العامة /الخاصة لإرسال المعلومات إلى الخادم. وتمنع هذه الطريقة ظهور مشاكل الاتصال مثل التجسُّس أو التنصُّت (eavesdropping) عند كشف المعلومات الحسّاسة (مثل: البيانات الشخصية، وأرقام بطاقات الائتمان (credit card)) ضمن أحد مواقع الويب.

ويُساعِد بروتوكول الطبقات الأمنية (SSL) في التحقُّق من المفتاح العام الذي أصدره الخادم، ويتأكَّد من عدم تغيُّر المعلومات أثناء النقل، وذلك باستخدام الشهادات الرقمية (digital certificates) التي سنتحدَّث عنها ضمن هذا البحث.

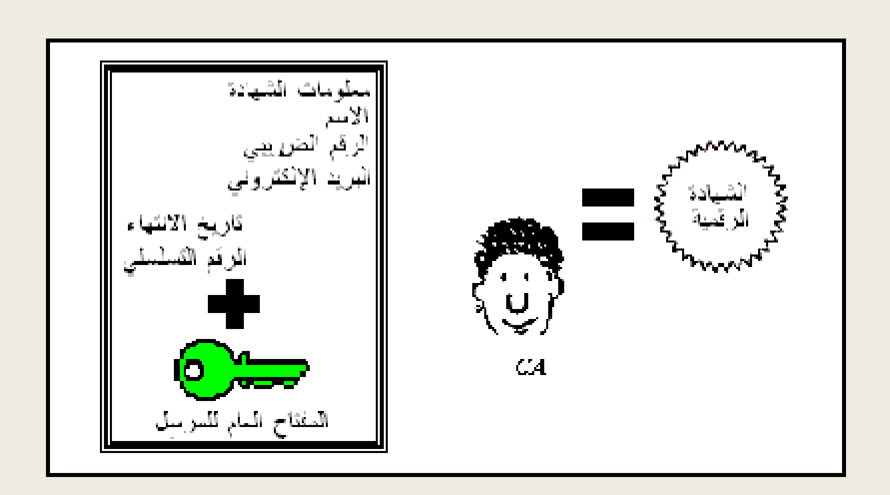
الشهادات الرقمية(Digital Certificates) :

ما هي الشهادات الرقمية؟

الشهادة الرقمية هي بمثابة رخصة قيادة أو جواز سفر أو أي شكل من أشكال إثبات الهوية.

تصدُر الشهادات الرقمية عن الجهات المانحة (certificate authorities- CA) الموثوق بها التي توقِّع عليها، وتُستَخدَم هذه الشهادات للتحقُّق من موثوقية المفاتيح العامة التي أُصدِرَت.

وفي البداية، يقوم شخص (أو شركة) بتوليد زوج من المفاتيح العامة/الخاصة، ثم يُرسَل المفتاح العام إلى جهة مانحة للشهادة (CA) .وتُضيف الجهة المانحة (CA) بعضَ المعلومات المتعلِّقة بالشهادة
(مثل: الاسم، ورقم التعريف(ID No) ، وعنوان البريد الإلكتروني(Email address) ، وتاريخ الانتهاء (expiration date)، والرقم التسلسُلي (serial no.))، وتُوقِّع عليها بالمفتاح العام لطالب الشهادة، وبالمفتاح الخاص للجهة المانحة للشهادة (CA) .ويصادِق توقيع الجهة المانحة للشهادة (CA) على المعلومات المُضافة إلى الشهادة وعلى المفتاح العام الموجود ضمن الشهادة. ويمكن أن ترسِل الجهةُ المانحةُ الشهادةَ إلى طالبها، أو تنشرَها للعموم، أو تحتفظَ بها في خادم الشهادات (certificate server) (و هو عبارة عن قاعدة بيانات تسمح بتسليم واسترجاع الشهادات الرقمية).
وَلِفكّ شيفرة الوثيقة المصدَّقة رقمياً(digitally certified document) ، تستخدِم البرمجياتُ في الطرف المستقبل المفتاحَ العام للجهة المانحة للشهادة(CA) ، فإن نجحت عملية فك شيفرة الشهادة، فإن ذلك يعني أن الجهة المانحة التي وقّعت الوثيقة هي التي أنشأتها بالفعل. وتستطيع البرمجياتُ في الطرف المستقبل أيضاً فحصَ جميع معلومات الشهادة المتعلِّقة بمالكها، مما يُمكِّن المستقبل من الحصول على المفتاح العام للمالك (من الشهادة) للتحقّق من توقيع المرسِل، فإن تمكَّن هذا المفتاح العام المُصدَّق من فك شيفرة توقيع المرسِل، يصبح المستقبل على ثِقةٍ بأن التوقيع أُنشِئ باستخدام المفتاح الخاص للمالك.



○ **أين يمكن الحصول على الشهادات الرقمية ؟**

يمكنك الحصول على شهادة رقمية من مرجع تجاري لإصدار الشهادات مثلVeriSign, Inc .أو من المسؤول عن الأمان الداخلي أو المسؤول عن تكنولوجيا المعلومات (IT)، أو يمكنك إنشاء التوقيع الرقمي بنفسك باستخدام الأداة Selfcert.exe.

ملاحظة:

بما أنه لا يتم إصدار الشهادة الرقمية التي تنشئها بنفسك من قبل مرجع مصدق رسمي، لذلك تتم الإشارة إلى المشاريع الموقعة باستخدام مثل هذه الشهادة على أنها مشاريع موقعة ذاتياً. تعتبر الشهادات التي تنشئها بنفسك غير مصدقة وستؤدي إلى إنشاء إنذار في المربع إنذار أمان إذا تم تعيين مستوى الأمان إلى مرتفع أو متوسط. سيثق فقط بشهادة موقعة ذاتياً على كمبيوتر يتوفر لديه المفتاح الخاص لتلك الشهادة (وبشكل عام فقط الكمبيوتر الذي أنشأ الشهادة فعلياً، إلا إذا تمت مشاركة المفتاح الخاص مع أجهزة كمبيوتر أخرى).

- **مراجع مصدقة تجارية :**

للحصول على شهادة رقمية من مرجع تجاري لإصدار الشهادات مثلVeriSign, Inc ،عليك أنت أو المؤسسة التقدم بطلب من ذلك المرجع.

عليك التقدم بطلب الحصول على شهادة رقمية من الفئة 2 أو الفئة 3 لناشري البرامج، وذلك يتوقف على وضعك كمطوّر:

الشهادة الرقمية من الفئة 2 مصمّمة للأشخاص الذين ينشرون البرامج بصفة فردية. وتوفر هذه الفئة من الشهادات الرقمية الثقة فيما يخص هوية الناشر .

الشهادة الرقمية من الفئة 3 مصمّمة للشركات والمؤسسات الأخرى التي تنشر البرامج. هذه الفئة من الشهادات الرقمية توفر ثقة أكبر فيما يخص هوية المؤسسة الناشرة. الشهادات الرقمية من الفئة 3 مصمّمة لتمثيل مستوى الثقة المتوفر حالياً بواسطة أقنية بيع البرامج. ويجب على المتقدم للحصول على شهادة رقمية من الفئة 3 أن يتمتع بالحد الأدنى من المستوى المالي الثابت استناداً إلى تصنيفات Dun & Bradstreet Financial Services

- **مراجع مصدقة داخلية :**

بإمكان بعض المؤسسات والشركات أن تعيّن شخصاً مسؤولاً عن الأمان أو مجموعة تعمل بصفة مرجع خاص بها لإصدار الشهادات، تنشئ أو توزع الشهادات الرقمية باستخدام أدوات مثلMicrosoft Certificate Server . وباستطاعة Microsoft Certificate Server العمل كمرجع مستقل لإصدار الشهادات أو جزء من تسلسل هرمي موجود لإصدار الشهادات. وحسب الطريقة التي يتم بها استخدام ميزات التواقيع الرقمية في مؤسستك، فقد تتمكّن من التوقيع على مشاريع الماكرو باستخدام شهادة رقمية صادرة عن مرجع داخلي في المؤسسة. أو قد تحتاج إلى مسؤول يقوم بالتوقيع على مشاريع الماكرو باستخدام شهادة تم التصديق عليها.

بعد تثبيت الشهادة الرقمية، يمكنك التوقيع على الملفات و مشاريع الماكرو.

التوقيع الرقمي على أحد الملفات يثبت أن المعلومات في الملف هي معلومات صالحة وبأنها لم تُعدّل منذ أن تم التوقيع على الملف. وباستطاعة المراجعين، طالما لم يطرأ أي تغيير على الملف، إرفاق توقيعهم به. ويمكنك أن تستخدم توقيعاً رقمياً للتوقيع على الملفات الهامة. وعند استخدام التوقيع الرقمي للتوقيع على مشروع ماكرو، يثبت التوقيع الرقمي سلامة المشروع. وكما أن الملفات الموقّعة تبقى كذلك حتى يتم تعديل الملف، فإن مشاريع الماكرو الموقّعة تبقى أيضاً كذلك إلى أن يتم تعديل التعليمات البرمجية للماكرو.

ملاحظة :

يمكن أن يتعرف الخادم على المستخدم عن طريق اسم المستخدم أو كلمة المرور أو PIN code و من المكن للمستخدم أيضا أن يمتلك و يستخدم الشهادات الرقمية و في هذه الحالة يسمى المستخدم **Client Side authentication** أي الموثوقية من جانب المستخدم مما يزيد من أمن الموقع.

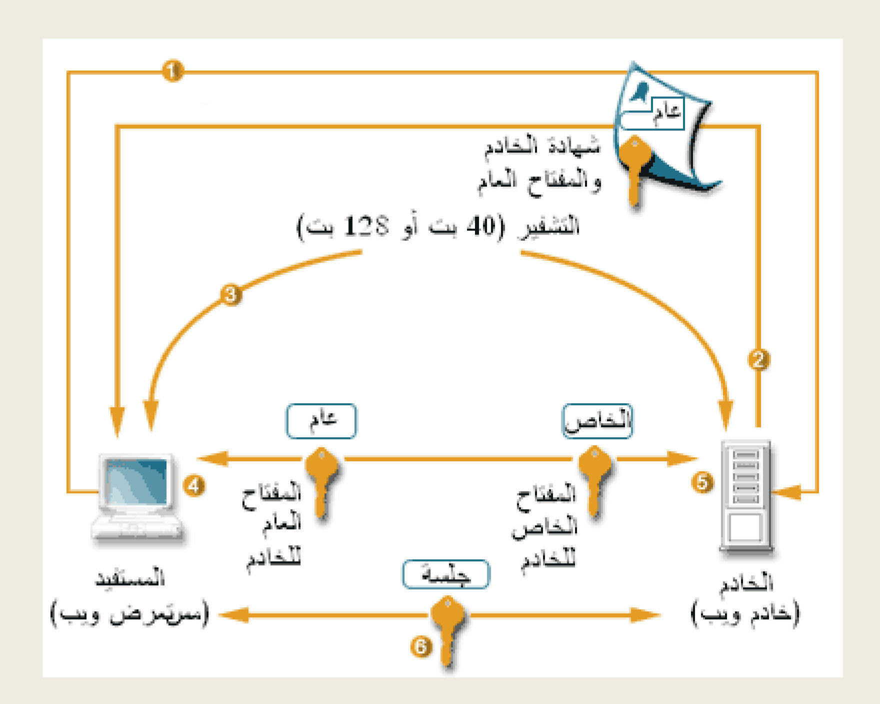
كيف يعمل بروتوكول الطبقات الأمنية(SSL) ؟

يُنشئ المستفيد اتصالاً بخادم آمن (secure server). ويُميَّز الخادم الآمن بإلحاق حرف "s" بنهاية اسم البروتوكول ضمن عنوان (URL)مثلاً(https://server.com) ، وبعد إنشاء الاتصال، يبدأ المستفيد جلسةَ المصافحة(SSL handshake session) ، وذلك بإرسال رسالة أو عبارة ترحيب (client hello) إلى الخادم تستفسر عن هوية الخادم وتخبره بقدرات التشفير لدى المستفيد (خوارزميات التشفير التي يمكنه تطبيقها). ويرُدُّ الخادم برسالة أو عبارة ترحيب(server hello) ، وإرسال **شهادته الرقمية** وبعض قوائم خوارزميات التشفير. ويقوم المستفيد بفحص الشهادة الرقمية للخادم، وذلك للتحقّق من أنها قد صدرت عن جهة مانحة (CA) معتَمَدة. ويقوم المستفيد أيضاً بفحص معلومات الشهادات الرقمية واسم الخادم والمفتاح العام. وبعد تحقُّق كل طرف من الطرف الآخر، يتَّفِق الخادم والمستفيد على معيار التشفير الذي سيُستَخدَم في جلسة تبادُل البيانات وفقاً لبروتوكول الطبقات الأمنية (SSL data exchange session).



المصافحة في جلسة بروتوكول الطبقات الأمنية

وبعد الانتهاء من جلسة المصافحة في بروتوكول الطبقات الأمنية(SSL) ، يولِّد المستفيد مفتاحاً سرياً للجلسة، ويشفِّره باستخدام المفتاح العام للخادم، ثم يفكّ الخادمُ شيفرةَ مفتاح الجلسة باستخدام مفتاحه الخاص. ويستخدِم كل من الخادم والمستفيد هذا المفتاح الفريد لتبادُل المعلومات الحساسة في جلسة بروتوكول الطبقات الأمنيّة. ولا يصلح هذا المفتاح الفريد إلا لجلسة واحدة فقط .



خبر عاجل ..!!

كسر طريقة صنع الشهادات الرقمية Site Certificates لمواقع الانترنت!!..

تمكنت مجموعة من الباحثين من كسر طريقة صنع الشهادات الرقمية والتي تستخدمها العديد من المواقع من أجل أن تثبت أنها مواقع آمنة ومعترف بها من قبل الشركات الأمنية .وكما أوضح الباحثون فإن المتصفح حين يقوم بالتعامل مع موقع يستخدم شهادة رقمية للتشفير فإنه يقوم بالتأكد من الجهة التي قامت بإصدار هذه الشهادة ومقارنتها مع قاعدة البيانات الخاصة بالشركات الموثوق بها، وقد تمكن الباحثون في تقديمهم من اختراق الشهادات التي تصدرها شركة Equifaxوهي أحد الشركات التي تقوم بإصدار الشهادات الرقمية الأمنية للمواقع حيث تعتبر هذه الشركة من الشركات الموثوق بها في مجال الشهادات الرقمية من قبل المتصفحات.



والعيب يكمن كما أوضح الباحثون في استخدام خوارزمية MD5 في التشفير حيث تعاني هذه الخوارزمية من ثغرة يستطيع المخترق أن يستغلها من أجل إنشاء شهادات رقمية مزيفة قد تستخدم في الاحتيال على المستخدم والاقتراح الوحيد الذي قدمه الباحثون للوقت الحالي هو استبدال خوارزمية MD5 في التشفير واستبدالها بطريقة جديدة أقوى لأجل المحافظة على مصداقية الشركات.

تم بعونه تعالى

M.N Moustafa-MN@hotmail.com

References:

- http://www.itep.ae/arabic/EducationalCenter/Articles/ssl_01.asp#2
- http://www.portsaid.gov.eg/forum2.aspx?g=posts&t=99
- http://forum.merkaz.net/t47172.html